Adam Pollock
POLLOCK COHEN LLP
111 Broadway, Suite 1804
New York, NY 10006
(212) 337-5361

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: (312) 621-2000

*pro hac vice forthcoming

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

MARK S. HOLDEN and RICHARD ANDISIO, individually, and on behalf of all others similarly situated, Plaintiffs, v. GUARDIAN ANALYTICS, INC., ACTIMIZE INC., and WEBSTER BANK, N.A., Defendants.	Case No. 23-2115 CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Mark S. Holden and Richard Andisio (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated (collectively, "Class members"), by and through their attorneys, bring this Class Action Complaint against Guardian Analytics, Inc. ("Guardian"), Actimize Inc. ("Actimize"), and Webster Bank, N.A. ("Webster Bank")

(collectively, "Defendants") and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to secure and safeguard their and at least 191,563 other individuals' personally identifiable information ("PII"), including names, Social Security numbers, and financial account numbers.

2. Guardian, which was acquired by Actimize in 2020, provides fraud detection services to Webster Bank. Actimize is a company that is owned by NICE Ltd.

3. Between November 27, 2022 and January 26, 2023, unauthorized individuals had access to Guardian's network systems and acquired the PII of Plaintiffs and Class members (the "Data Breach").

4. Defendants owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect their PII from unauthorized access and disclosure.

5. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all persons whose PII was exposed as a result of the Data Breach.

6. Plaintiffs, on behalf of themselves and all other Class members, assert claims for negligence, negligence per se, breach of implied contract, unjust enrichment, and violations of the Connecticut Unfair Trade Practices Act, and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Mark S. Holden

7. Plaintiff Mark S. Holden is a citizen of the State of Connecticut.

8. Plaintiff Holden was required to provide his PII to Webster Bank in connection with using banking services from Webster Bank.

9. Based on representations made by Webster Bank, Plaintiff Holden believed that Webster Bank had implemented and maintained reasonable security and practices to protect his PII. With this belief in mind, Plaintiff Holden provided his PII to Webster Bank in connection with or in exchange for banking services.

10. In connection with services provided to Plaintiff Holden, Defendants store and maintain Plaintiff's PII on their systems, including the system involved in the Data Breach.

11. Had Plaintiff Holden known that Defendants do not adequately protect the PII in their possession, he would not have agreed to provide Webster Bank with his PII.

12. Plaintiff Holden received letters from Webster Bank, including one notifying him that his PII was exposed in the Data Breach and two notifying him that his businesses' information was exposed in the Data Breach.

13. As a direct result of the Data Breach, Plaintiff Holden has suffered injury

and damages including, *inter alia*: a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII; deprivation of the value of his PII; and overpayment for services that did not include adequate data security.

Plaintiff Richard Andisio

14. Plaintiff Richard Andisio is a citizen of the State of Connecticut.

15. Plaintiff Andisio was required to provide his PII to Webster Bank in connection with using banking services from Webster Bank.

16. Based on representations made by Webster Bank, Plaintiff Andisio believed that Webster Bank had implemented and maintained reasonable security and practices to protect his PII. With this belief in mind, Plaintiff Andisio provided his PII to Webster Bank in connection with or in exchange for banking services.

17. In connection with services provided to Plaintiff Andisio, Defendants store and maintain Plaintiff's PII on their systems, including the system involved in the Data Breach.

18. Had Plaintiff Andisio known that Defendants do not adequately protect the PII in their possession, he would not have agreed to provide Webster Bank with his PII.

19. Plaintiff Andisio received a letter from Webster Bank notifying him that his PII was exposed in the Data Breach.

20. As a direct result of the Data Breach, Plaintiff Andisio has suffered injury and damages including, *inter alia*: a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII; deprivation of

the value of his PII; and overpayment for services that did not include adequate data security.

Defendants

21. Defendant Guardian Analytics, Inc. is a corporation that was formed under the laws of Delaware. Guardian Analytics' principal place of business is located at 221 River St., Hoboken, NJ 07030. Defendant Guardian Analytics can be served via its Registered Agent, Corporation Service Company, 251 Little Falls Drive, Wilmington, DE, 19808.

22. Defendant Actimize Inc. is a corporation that was formed under the laws of Delaware. Actimize's principal place of business is located at 221 River St., Hoboken, NJ 07030. Defendant Actimize can be served via its Registered Agent, Corporation Service Company, 251 Little Falls Drive, Wilmington, DE, 19808.

23. Defendant Webster Bank, N.A. is a national bank that has its principal place of business in Connecticut. Webster Bank is headquartered at 200 Elm St., Stamford, CT 06902. Webster Bank can be served at its principal place of business.

JURISDICTION AND VENUE

24. The Court has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

25. This Court has personal jurisdiction over Defendants Guardian and Actimize because Guardian and Actimize have their principal place of business in New

Jersey. The Court has personal jurisdiction over Defendant Webster Bank because Webster Bank contracts with Guardian, a company headquartered in New Jersey, and therefore purposely availed itself to the laws of New Jersey.

26. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Defendants Guardian and Actimize have their principal place of business in Hudson County, New Jersey, and a substantial part of the events giving rise to Plaintiffs' claims arose in this District.

FACTUAL ALLEGATIONS

Overview of Defendants

27. Guardian is a company that provides "behavioral analytics and machine learning solutions for preventing banking fraud and anti-money laundering."[1] Guardian was acquired by Actimize, which claims to be the "largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions."[2]

28. Webster Bank is a "commercial bank that delivers financial solutions to businesses, individuals, families and partners."[3] The company claims to control over $70 billion in assets.[4]

---

[1] *About Guardian Analytics*, GUARDIAN ANALYTICS, https://guardianananalytics.com/about-guardian-analytics/ (last accessed Apr. 14, 2023).

[2] *Id.*

[3] *About*, WEBSTER BANK, https://public.websteronline.com/about (last accessed Apr. 14, 2023).

[4] *Id.*

29. Guardian provides Webster Bank with "fraud detection services."[5] Webster Bank provided Guardian with its customers' PII in exchange for these services.

30. In the regular course of their business, Defendants collect and maintain the PII of their clients and their clients' customers.

31. Guardian's website contains a privacy policy regarding the data it collects through its website which states: "The privacy and protection of your personal information is important to us. We follow generally accepted industry standards to protect the personal information submitted to us, both during transmission and once we receive it."[6]

32. Actimize's website contains a privacy policy regarding the data it collects through its website which states, "Your privacy is important to us," and goes on to state, "[Actimize] implements data security systems and procedures to secure the information stored on [Actimize] computer servers."[7]

33. Webster Bank has a page on its website dedicated to customer privacy. The page states, among other representations, "We take the privacy and security of your

[5] *See Notice of Data Breach*, WEBSTER BANK, https://apps.web.maine.gov/online/aeviewer/ME/40/a42f73e8-720b-41a2-b892-18181e799668/25a99f73-65d3-4c27-bea6-9440850e90c7/document.html (last accessed Apr. 14, 2023).

[6] *Privacy Policy*, GUARDIAN ANALYTICS, https://guardiananalytics.com/privacy-policy/ (last accessed Apr. 14, 2023).

[7] *NICE Privacy Notice*, ACTIMIZE, https://www.nice.com/company/legal/privacy-policy (last accessed Apr. 14, 2023).

information seriously and our number one goal is to give you peace of mind when it comes to your protection."[8]

34. Plaintiffs and Class members are, or were, customers of a Webster Bank and entrusted Defendants with their PII.

The Data Breach

35. Between November 27, 2022 and January 22, 2023, unauthorized individuals had access to Guardian's network systems.[9] Those unauthorized individuals acquired the PII of Plaintiffs and Class members and posted the information on the internet.[10] This has left all of Plaintiffs and Class members at an imminent risk of fraud and identity theft, if they have not already experienced them.

36. Guardian notified Webster Bank of the Data Breach on January 26, 2023.[11] However, Webster Bank did not begin reporting the Data Breach to Plaintiffs, Class members, and state authorities until on or about April 10, 2023. Thus, Plaintiffs' and Class members' PII was in the hands of cybercriminals for over two months before they were warned that the Data Breach affected this information.

37. The notice that Webster Bank sent to those affected by the Data Breach states the information that was disclosed included a person's "name, Social Security number, and financial account number."[12]

---

[8] *Safety and Security*, Webster Bank, https://public.websteronline.com/security (last accessed Apr. 14, 2023).

[9] *See Notice of Data Breach*, n.5, *supra*.

[10] *Id.*

[11] *Id.*

[12] *Id.*

Defendants Knew that Criminals Target PII

38. At all relevant times, Defendants knew, or should have known, that the PII that they collected was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII from cyber-attacks that Defendants should have anticipated and guarded against.

39. It is well known among companies that store sensitive personally identifying information that such information—such as the Social Security numbers ("SSNs") and financial information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers …. Many of them were caused by flaws in … systems either online or in stores."[13]

40. PII is a valuable property right.[14] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[15] American

---

[13] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[14] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

[15] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[16] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

41. As a result of the real and significant value of these data, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

42. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[17]

43. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[16] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[17] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

Theft of PII Has Grave and Lasting Consequences for Victims

44. Theft of PII can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[18]

45. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[19] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to, among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[20]

---

[18] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Apr. 14, 2023).

[19] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[20] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/ (last accessed Apr. 14, 2023).

46. With access to an individual's PII, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: opening utility accounts using the victim's identity; file a fraudulent tax return using the victim's information; or even give the victim's personal information to police during an arrest.[21]

47. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[22]

48. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

49. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (*e.g.*, name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[23]

---

[21] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Apr. 14, 2023).

[22] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Apr. 14, 2023).

[23] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

50. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a victim discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some victims up to three years to learn that information.[24]

51. It is within this context that Plaintiffs and Class members must now live with the knowledge that their PII is forever in cyberspace, having been stolen by criminals willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

Damages Sustained by Plaintiffs and the Other Class members

52. Plaintiffs and Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft—risk which justifies or necessitates expenditures for protective and remedial services, for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

CLASS ACTION ALLEGATIONS

53. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23.

---

[24] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

54. Plaintiffs bring this action on behalf of themselves and all members of the following Class of similarly situated persons:

> All persons whose personally identifiable information was accessed in the Data Breach by unauthorized persons, including all who were sent a notice of the Data Breach.

55. Excluded from the Class are Guardian Analytics, Inc., Actimize Inc., Webster Bank, N.A., and their affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

56. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

57. The members of the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. Webster Bank reported to the Maine Attorney General that approximately 191,563 of its customers' information was exposed in the Data Breach.[25]

58. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class members' PII from unauthorized access and disclosure;

[25] *Data Breach Notifications*, OFF. OF THE MAINE ATT'Y GEN., https://apps.web.maine.gov/online/aeviewer/ME/40/a42f73e8-720b-41a2-b892-18181e799668.shtml (last accessed Apr. 14, 2023).

b. whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' PII;

c. whether an implied contract existed between Class members and Defendants, providing that Defendants would implement and maintain reasonable security measures to protect and secure Class members' PII from unauthorized access and disclosure;

d. whether Defendants breached their duties to protect Plaintiffs' and Class members' PII; and

e. whether Plaintiffs and Class members are entitled to damages and the measure of such damages and relief.

59. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

60. Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiffs and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

61. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or that conflict with, the Class they seek to represent. Plaintiffs

have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

62. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

63. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

64. Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting the PII in Defendants' possession, custody, or control.

65. Defendants knew or should have known the risks of collecting and storing Plaintiffs' and Class members' PII and the importance of maintaining secure systems. Defendants knew or should have known that they faced an increased threat of customer data theft, as judged by the many data breaches that targeted companies that stored PII in recent years.

66. Given the nature of Defendants' business, the sensitivity and value of the PII they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

67. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs and Class members' PII by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiffs' and Class members' PII.

68. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII to unauthorized individuals.

69. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiffs and Class members, their PII would not have been compromised.

70. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risk justifying or necessitating expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

71. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

72. Defendants' duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair … practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Defendants, of failing to employ reasonable measures to protect and secure PII.

73. Defendants' violation of Section 5 of the FTCA constitutes negligence per se.

74. Plaintiffs and Class members are within the class of persons that Section 5 of the FTCA was intended to protect.

75. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiffs and Class members as a result of the Data Brach.

76. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PII to unauthorized individuals.

77. The injury and harm that Plaintiffs and Class members suffered was the direct and proximate result of Defendants' violations of Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risk justifying or necessitating expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach,

including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF IMPLIED CONTRACT
(Against Webster Bank)

78. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

79. Plaintiffs bring this claim only against Webster Bank.

80. In connection with the dealings Plaintiffs and Class members had with Defendants, Plaintiffs and Class members entered into implied contracts with Webster Bank.

81. Pursuant to these implied contracts, Plaintiffs and Class members provided Webster Bank with their PII, directly or indirectly, in order for Webster Bank to provide services. In exchange, Webster Bank agreed to, among other things, and Plaintiffs and Class members understood that Webster Bank would: (1) provide services to Plaintiffs and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII; and (3) protect Plaintiffs' and Class members' PII in compliance with federal and state laws and regulations and industry standards.

82. The protection of PII was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and Webster Bank, on the other hand. Indeed, Webster Bank was clear in its representations regarding privacy, and on that basis of those representations Plaintiffs understood that Webster Bank supposedly respects and is committed to protecting customer privacy.

83. Had Plaintiffs and Class members known that Webster Bank would not adequately protect its customers' and former customers' PII, they would not have provided Webster Bank with their PII.

84. Plaintiffs and Class members performed their obligations under the implied contracts when they provided Webster Bank with their PII, either directly or indirectly.

85. Webster Bank breached its obligations under its implied contracts with Plaintiffs and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

86. Webster Bank's breach of its obligations of the implied contracts with Plaintiffs and Class members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

87. Plaintiffs and all other Class members were damaged by Webster Bank's breach of implied contracts because: (i) they paid—directly or indirectly—for data security protection they did not receive; (ii) they face a substantially increased and imminent risk of identity theft—a risk justifying or necessitating expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; and (vi) lost time and money

incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

COUNT IV
UNJUST ENRICHMENT

88. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

89. This claim is pleaded in the alternative to the breach of implied contract claim.

90. Plaintiffs and Class members conferred a monetary benefit upon Defendants in the form of monies paid for services to Webster Bank, who then used these funds to pay Guardian and Actimize.

91. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiffs and Class members. Defendants also benefitted from the receipt of Plaintiffs' and Class members' PII, as this was used in providing banking or other services.

92. As a result of Defendants' conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

93. Defendants should not be permitted to retain the money belonging to Plaintiffs and Class members because Defendants failed to adequately implement the data privacy and security procedures for themselves that Plaintiffs and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

94. Defendants should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
VIOLATIONS OF THE CONNECTICUT UNFAIR TRADE PRACTICES ACT
Conn. Gen. Stat. §§ 42-110a, *et seq*. ("CUTPA")

95. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

96. CUTPA states, "No person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Conn. Gen Stat. § 42-110b.

97. Plaintiffs, Class members, and Defendants are "persons" under CUTPA. Conn. Gen Stat. § 42-110a.

98. The services that Defendants provide are "trade" and "commerce" pursuant to CUTPA. Conn. Gen Stat. § 42-110a.

99. Webster Bank made representations to Plaintiffs and Class members that their PII will remain private, as evidenced by, *inter alia*, its representations regarding privacy on its website. Webster Bank committed deceptive acts in violation of CUTPA by failing to inform Plaintiffs and Class members that Webster Bank would not adequately secure Plaintiffs' and Class members' PII by contracting with parties that did not have adequate safeguards in place to protect PII.

100. All Defendants engaged in unfair acts in violation of CUTPA by failing to implement and maintain reasonable security measures to protect and secure Plaintiffs' and Class members' PII in a manner that complied with applicable laws, regulations, and

industry standards. The failure to implement and maintain reasonable data security measures offends established public policy, is immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

101. Due to the Data Breach, Plaintiffs and Class members have lost property in the form of their PII. Further, Defendants' failure to adopt reasonable practices in protecting and safeguarding their customers' PII will force Plaintiffs and Class members to spend time or money to protect against identity theft. Plaintiffs and Class members are now at a higher risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Defendants' practice of collecting and storing PII without appropriate and reasonable safeguards to protect such information.

102. Plaintiffs and all other Class members were damaged by Defendants' violation of CUTPA because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased and imminent risk of identity theft—a risk justifying or necessitating expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) they overpaid for the services that were received without adequate data security.

PRAYER FOR RELIEF

Plaintiffs, individually, and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against Defendants as follows:

A. certifying the Class as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. awarding Plaintiffs and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: April 14, 2023

Respectfully submitted,

/s/ *Adam Pollock*
Adam Pollock
POLLOCK COHEN LLP
111 Broadway, Suite 1804
New York, NY 10006
Tel: (212) 337-5361
adam@pollockcohen.com

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: (312) 621-2000
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

*pro hac vice forthcoming

Attorneys for Plaintiffs and the Proposed Class